AMENDMENTS TO CLAIMS

This listing of claims replaces all prior versions and listings of claims:

1. (Previously presented) An information storage medium (ISM) comprising means storing:

an encrypted content;

encryption key information needed in a process of decoding the encrypted content;

an associated ISM ID, said associated ISM ID being an identifier uniquely assigned to the ISM; and

a first list identifying revoked ISM ID's, said first list having an associated first version date and an associated tampering check value for checking whether said first list is untampered,

wherein,

the ISM is adapted for operation with an information processing apparatus, said apparatus having

means for executing a process for playing back content stored on the ISM,

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date,

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in said second list,

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in said second list,

means for checking the associated tampering check value to determine whether

the first list identifying revoked ISM ID's is untampered, and

means for updating said memory, by replacing said second list with the first list, said means for updating said memory enabled to only operate when the first list is untampered and the associated first version date is later than said associated second version date.

2. (Previously Canceled).

3. (Previously presented) The information storage medium according to claim 1, wherein the encryption key information includes an enabling key block (EKB) as encryption key data from which a key used to decrypt the encrypted content is extractable.

4. (Previously presented) The information storage medium according to claim 3, wherein the enabling key block (EKB) is encryption key information that can be decrypted based on a device node key (DNK) provided in the form of a hierarchical key-distribution tree structure to an information processing apparatus that is a device using the information storage medium.

5. (Previously presented) An information processing apparatus comprising:

means for executing a process for playing back content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date;

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date;

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for disabling the process for playing back content when the associated ISM ID is identical

to a revoked ISM ID identified in the second list;

means for performing a tampering check process to check whether the first list identifying revoked ISM ID's is untampered; and

means for updating the memory, by replacing the second list with the first list, said means enabled to only operate when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.

6. (Previously Canceled)

7. (Previously presented) The information processing apparatus according to claim 5, wherein: the information processing apparatus has a device node key (DNK) as key information provided in the form of a hierarchical key-distribution tree structure; and a key used to decrypt an encrypted content stored on the information storage medium is extracted by decoding, based on the device node key (DNK), an enabling key block (EKB) stored as encryption key information on the information storage medium.

8. (Previously presented) An information storage medium (ISM) production system comprising:

means for producing a plurality of ISM's and storing information on at least one ISM, said information comprising:

an encrypted content, encryption key information needed in a process of decoding the encrypted content, a first list identifying revoked ISM ID's, said first list having an associated first version date and an associated tampering check value for checking whether the first list is untampered, and an associated ISM ID, said associated ISM ID being an identifier uniquely assigned to each ISM;

wherein, the at least one ISM is adapted for operation with an information processing apparatus, said apparatus having:

means for executing a process for playing back content stored on the ISM;

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date;

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for checking the associated tampering check value to determine whether the first list identifying revoked ISM ID's is untampered; and

means for updating the memory, by replacing the second list with the first list, said means for updating the memory enabled to only operate when the first list is untampered and the associated first version date is later than the associated second version date.

9. (Previously Canceled)

10. (Previously presented) The information storage medium production apparatus according to claim 8, wherein the encryption key information includes an enabling key block (EKB) as encryption key data to be applied in the decryption of the encrypted content.

11. (Previously presented) An information processing method comprising the steps of:

executing, with an information processing apparatus, a process for playing back content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date, said executing step further comprising:

reading the associated ISM ID;

checking whether the associated ISM ID is identical to a revoked ISM ID identified in a second list identifying revoked ISM ID's, said second list having an associated second version date, and said second list being stored in a memory of the information processing apparatus;

disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

performing a tampering check process to check whether the first list identifying revoked ISM ID's is untampered; and

updating the memory of the information processing apparatus, by replacing the second list with the first list, only when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.

12. (Previously Canceled)

13. (Previously presented) The information processing method according to claim 11, further comprising the step of acquiring a key used to decode an encrypted content stored on the information storage medium by decoding an enabling key block (EKB) stored as encryption key information on the information storage medium, the decoding of the enabling key block (EKB) being based on a device node key (DNK) provided as key information provided in the form of a hierarchical key-distribution tree structure.

14. (Previously presented) An information storage medium (ISM) production method, comprising:

producing a plurality of ISM's and storing information on at least one ISM, said information comprising:

an encrypted content, encryption key information needed in a process of decoding the encrypted content, a first list identifying revoked ISM ID's said first list having an associated first version

date and an associated tampering check value for checking whether the first list is untampered, and an associated ISM ID, said associated ISM ID being an identifier uniquely assigned to each ISM;

wherein, the at least one ISM is adapted for operation with an information processing apparatus, said apparatus having:

means for executing a process for playing back content stored on the ISM;

a memory for storing a second list identifying revoked ISM ID's, said second list having an associated second version date;

means for checking whether the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

means for checking the associated tampering check value to determine whether the first list identifying revoked ISM ID's is untampered; and

means for updating the memory, by replacing the second list with the first list, said means for updating the memory enabled to only operate when the first list is untampered and the associated first version date is later than the associated second version date.

15. (Currently Amended) A computer storage medium encoded with a computer program for executing a process for playing back content stored on an information storage medium (ISM), wherein both an associated ISM ID and a first list identifying revoked ISM ID's are stored on said ISM, said first list having an associated first version date, said process comprising the steps of:

reading the associated ISM ID;

checking whether the associated ISM ID is identical to a ISM ID identified in a second list identifying revoked ISM ID's, said second list having an associated second version date, and said second list being stored in a memory of the information processing apparatus;

disabling the process for playing back content when the associated ISM ID is identical to a revoked ISM ID identified in the second list;

performing a tampering check process to check whether the first list identifying revoked ISM ID's is untampered; and

updating the memory of the information processing apparatus, by replacing the second list with the first list, only when both: the tampering check process determines that the first list is untampered; and, the associated first version date is later than the associated second version date.